UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,001	07/05/2001	Mark J. McArdle	002114.P021	5140

28875 7590 06/16/2006

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 06/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/900,001	MCARDLE ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-14,16-26 and 28-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-14,16-26 and 28-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 17 May 2006.

2. Claims 1, 2, 4-14, 16-26 and 28-43 are pending in the application.

3. Claims 1, 2, 4-14, 16-26 and 28-43 have been rejected.

4. Claims 3, 15 and 27 have been cancelled.

Response to Amendment

5. Applicant's request for reconsideration of the finality of the rejection of the last Office action is persuasive and, therefore, the finality of that action is withdrawn.

Response to Arguments

6. Applicant's arguments with respect to claims 1, 2, 4-14, 16-26 and 28-39 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 2, 4-14, 16-26 and 28-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vairavan US 2002/0083344 A1 in view of Drake U.S. Patent No. 6,006,328.

As to claims 1, 5, 40 and 41, Vairavan discloses intercepting a portion of outgoing network data [0131].

Vairavan does not teach conditionally masking the portion of outgoing network data to impersonate a different operating system in accordance with a security policy if the network is an untrusted network. Vairavan does not teach replacing the portion of outgoing network data with data characteristic of the different operating system.

Drake teaches impersonating a different operating system [column 4 line 47 to column 5 line 34]. Drake teaches replacing data with data characteristic of the different operating system [column 4 line 47 to column 5 line 34]. Drake teaches impersonating any one of the plurality of different operating systems [column 14, lines 33-39].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vairavan so that the firewall would have intercepted a portion of outgoing network data that had characteristics of a particular operating system. The firewall would have conditionally masked the portion of outgoing network data to impersonate a different operating system in accordance with a security policy if the network is an untrusted network. The replacement of the outgoing network data would have been used to prevent identification of the operating system for misleading attackers into attempting attacks that are unworkable on the operating system. The system would have been able to impersonate any one of a plurality of different operating systems.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vairavan by the teaching of Drake because certain operating system more vulnerable to attacks. Therefore, if it were an untrusted network, you would not want an outsider to penetrate your operating system.

As to claims 2, 14, 26 and 43, Vairavan teaches discarding the portion of outgoing network data [0132].

As to claims 4 and 16, Vairavan teaches that the security policy identifies the portion of outgoing network data and specifies an action to take to mask the portion of outgoing network data [0085].

As to claims 6, 18 and 39, Vairavan teaches that the security policy further defines the network as untrusted [0134-0135].

As to claims 7, 19 and 29, Vairavan teaches receiving the security policy through the network [0134-0135].

As to claims 8, 20 and 30, Vairavan teaches modifying the security policy based on user input [0066-0067].

As to claims 9, 21 and 28, Vairavan teaches transmitting the portion of outgoing network data unchanged if the network is a trusted network [0074].

As to claims 12, 24 and 32, Vairavan teaches that the method is integrated into a firewall that protects the computer [0085].

As to claims 13 and 17, Vairavan discloses intercepting a portion of outgoing network data [0131].

Vairavan does not teach conditionally masking the portion of outgoing network data to impersonate a different operating system in accordance with a security policy if the network is an untrusted network. Vairavan does not teach replacing the portion of outgoing network data with data characteristic of the different operating system.

Drake teaches impersonating a different operating system [column 4 line 47 to column 5 line 34]. Drake teaches replacing data with data characteristic of the different operating system [column 4 line 47 to column 5 line 34]. Drake teaches impersonating any one of the plurality of different operating systems [column 14, lines 33-39].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vairavan so that the firewall would have intercepted a portion of outgoing network data that had characteristics of a particular operating system. The firewall would have conditionally masked the portion of outgoing network data to impersonate a different operating system in accordance with a security policy if the network is an untrusted network. The replacement of the outgoing network data would have been used to prevent identification of the operating system for misleading attackers into attempting attacks that are unworkable on the operating system. The system would have been able to impersonate any one of a plurality of different operating systems.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vairavan by the teaching of Drake because certain operating system more vulnerable to attacks. Therefore, if it were an untrusted network, you would not want an outsider to penetrate your operating system.

As to claims 10, 22, 31, 37 and 38, the Vairavan-Drake combination teaches the method further comprising:

> intercepting a portion of incoming network data, as discussed above; and
>
> sending a false response to the portion of incoming network data to impersonate the different operating system in accordance with the security policy if the network is an untrusted network [Drake column 8, lines 24-63].

As to claims 11 and 23, the Vairavan teaches that the security policy identifies the portion of incoming network data and the false response [column 0074-0080].

As to claims 25 and 33, Vairavan discloses intercepting a portion of outgoing network data [0131].

Vairavan does not teach conditionally masking the portion of outgoing network data to impersonate a different operating system in accordance with a security policy if the network is an untrusted network. Vairavan does not teach replacing the portion of outgoing network data with data characteristic of the different operating system.

Drake teaches impersonating a different operating system [column 4 line 47 to column 5 line 34]. Drake teaches replacing data with data characteristic of the different operating system [column 4 line 47 to column 5 line 34]. Drake teaches impersonating any one of the plurality of different operating systems [column 14, lines 33-39].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vairavan so that the firewall would have intercepted a portion of outgoing network data that had characteristics of a particular operating system. The firewall would have conditionally masked the portion of outgoing network data to

impersonate a different operating system in accordance with a security policy if the network is an untrusted network. The replacement of the outgoing network data would have been used to prevent identification of the operating system for misleading attackers into attempting attacks that are unworkable on the operating system. The system would have been able to impersonate any one of a plurality of different operating systems.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vairavan by the teaching of Drake because certain operating system more vulnerable to attacks. Therefore, if it were an untrusted network, you would not want an outsider to penetrate your operating system.

As to claims 34-36, Vairavan discloses intercepting a portion of outgoing network data [0131].

Vairavan does not teach conditionally masking the portion of outgoing network data to impersonate a different operating system in accordance with a security policy if the network is an untrusted network. Vairavan does not teach replacing the portion of outgoing network data with data characteristic of the different operating system.

Drake teaches impersonating a different operating system [column 4 line 47 to column 5 line 34]. Drake teaches replacing data with data characteristic of the different operating system [column 4 line 47 to column 5 line 34]. Drake teaches impersonating any one of the plurality of different operating systems [column 14, lines 33-39].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vairavan so that the firewall would have intercepted a portion of outgoing network data that had characteristics of a particular operating

system. The firewall would have conditionally masked the portion of outgoing network data to impersonate a different operating system in accordance with a security policy if the network is an untrusted network. The replacement of the outgoing network data would have been used to prevent identification of the operating system for misleading attackers into attempting attacks that are unworkable on the operating system. The system would have been able to impersonate any one of a plurality of different operating systems.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vairavan by the teaching of Drake because certain operating system more vulnerable to attacks. Therefore, if it were an untrusted network, you would not want an outsider to penetrate your operating system.

As to claim 42, Vairavan teaches that the false response is sent if the operating system would normally not respond to the incoming network data [0131].

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy
June 8, 2006